



19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

12 Offenlegungsschrift
10 DE 199 22 155 A 1

51 Int. Cl.⁷:
G 06 F 12/14
G 06 K 19/073_

21 Aktenzeichen: 199 22 155.3
22 Anmeldetag: 12. 5. 1999
43 Offenlegungstag: 23. 11. 2000

DE 199 22 155 A 1

71 Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

72 Erfinder:
Baldischweiler, Michael, 81929 München, DE;
Eckardt, Stefan, 81739 München, DE

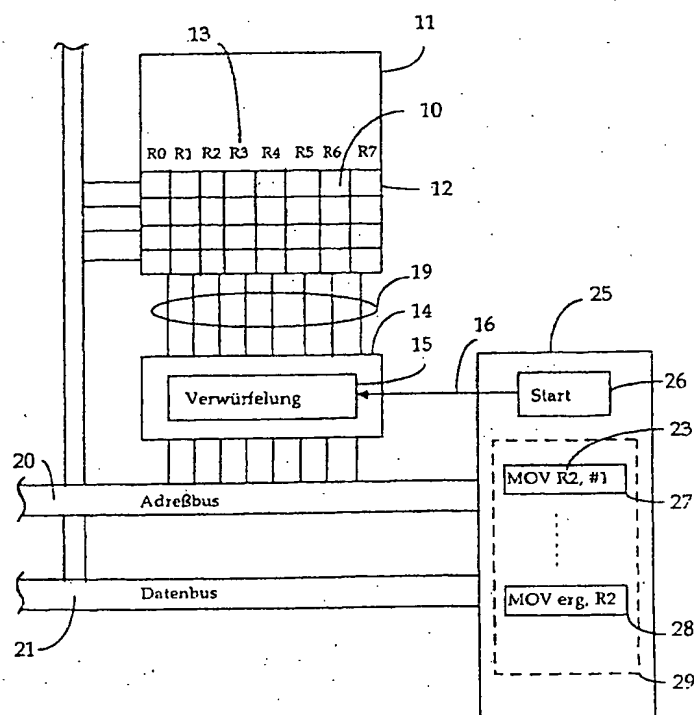
56 Entgegenhaltungen:
GB 22 48 702 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

54 Speicheranordnung mit Adreßverwürfelung

57 Vorgeschlagen wird eine Speicheranordnung mit einem Speicher mit einer Vielzahl von Speicherzellen (10) sowie einer Auswahlrichtung (14), die aufgrund einer über einen Adreßbus (20) zugeführten logischen Adresse (23) eine Speicherzelle (10) für einen physikalischen Zugriff auswählt. Die Auswahlrichtung (14) beinhaltet eine Verwürfelungsvorrichtung (15), die einer der Auswahlrichtungen (14) übermittelten logischen Adresse (23) durch Verwürfelung in vorhersehbarer Weise eine Speicherzelle (10) in der Speicheranordnung zuordnet, auf die anschließend der physikalische Zugriff erfolgt.



DE 199 22 155 A 1

Beschreibung

Die Erfindung geht aus von einer Speicheranordnung nach der Gattung des Hauptanspruchs. Speicheranordnungen dieser Art sind Bestandteil aller gängigen Mikrocomputer und u. a. in "Chip und System" R. Zaks, SYBEX-Verlag, 1984, Seite 133 ff. beschrieben. Grundsätzlich gleichartige Mikrocomputer werden auch in sicherheitsrelevanten Anwendungen, etwa in Chipkartensystemen zur Durchführung von Finanztransaktionen, eingesetzt. Allerdings werden in diesen Fällen regelmäßig zusätzliche Maßnahmen ergriffen, um Angriffe auf die Sicherheit durch Manipulation des Mikrocomputers zu verhindern. Ein Beispiel hierfür für eine solche Maßnahme findet sich in "Chipkarten", Karlheinz Fietta, Hüthig Verlag, 1989, Seiten 68 bis 72. Bei dem darin beschriebenen Chip TS 1834 der Firma THOMSON sind der Adreß- und Datenbus mittels eines Interfaces nach außen hin unsichtbar gemacht. Eine andere Maßnahme zur Erhöhung der Manipulationssicherheit des Mikrocomputers ist aus EP 694 846 A1 entnehmbar. Danach ist vorgesehen, die über den Datenbus übertragenen Daten gegebenenfalls mehrfach zu verwürfeln, so daß eine Auswertung und damit eine Manipulation der Daten selbst dann nicht möglich ist, wenn es gelingt, sie auszulesen.

Obgleich bereits die bekannten Maßnahmen ein hohes Maß an Sicherheit gewährleisten, ist es mit Blick auf die besondere Bedeutung der Sicherheit von im Zusammenhang mit der Ausführung von Finanztransaktionen eingesetzten Mikrocomputern wünschenswert, deren Manipulationssicherheit weiter zu verbessern. Der Erfindung liegt die Aufgabe zugrunde, weitere dieses leistende Maßnahmen anzugeben.

Diese Aufgabe wird gelöst durch eine Anordnung sowie ein Verfahren mit den Merkmalen der unabhängigen Ansprüche 1 und 7. Erfindungsgemäß wird wenigstens einem im Mikrocomputer vorhandenen Speicher mit wahlfreiem Zugriff eine Verwürfelungseinrichtung vorgeschaltet, welche den über den Adreßbus übermittelten logischen Adressen in unvorhersehbarer Weise physikalisch darauf tatsächlich belegte Zellen im Speicher zuordnet. Die erfindungsgemäße Speicheranordnung bietet dadurch den Vorteil, daß eine Manipulation des Mikrocomputers durch Analyse der Inhalte der Speicherzellen des Speichers mit wahlfreiem Zugriff unmöglich wird. Die zur Realisierung der Verwürfelungseinrichtung benötigte Logik verbraucht wenig Platz und läßt sich ohne weiteres in laufende Mikrocomputerfertigungen einbeziehen. Bevorzugt wird die Verwürfelung auf definierte Ereignisse hin regelmäßig erneuert.

Unter Bezugnahme auf die Zeichnung wird nachfolgend ein Ausführungsbeispiel der Erfindung näher erläutert.

Die Figur zeigt eine Speicheranordnung eines Mikrocomputers.

Fig. 1 zeigt als Ausschnitt aus der Gesamtstruktur eines Mikrocomputers dessen Speicheranordnung. Bezugszahl 11 bezeichnet dabei einen Speicher mit wahlfreiem Zugriff, d. h. in der Regel einen flüchtigen, oder zunehmend auch nicht flüchtigen RAM-Speicher, welcher in eine Vielzahl von Registerbänken 12 gegliedert sein kann. Jede Registerbank 12 gliedert sich ihrerseits in eine definierte Zahl von Speicherzellen 10, deren physikalische Position innerhalb einer Registerbank 12 jeweils durch eine zugeordnete Adresse 13 eindeutig bezeichnet ist. Jede Speicherzelle 10 speichert eine Information von einem Byte, eine Registerbank 12 beinhaltet üblicherweise acht Speicherzellen 10 oder ein ganzzahliges Vielfaches davon.

Der Speicher 11 ist über einen Datenbus 21 mit einem Mikrocontroller 25 verbunden. Dessen wesentliche Funktion ist die Ausführung von Programmbefehlen, welche in übli-

cher Weise in einer vorzugsweise nichtflüchtigen, nicht weiter beschriebenen Speichereinrichtung abgelegt sind. Die Abarbeitung der Programmbefehle beinhaltet Schreib- und Lesezugriffe auf den Speicher 11. Über den Datenbus 21 erfolgt dabei der Transport der in die Registerbänke 12 einzuschreibenden bzw. auszulesenden Dateninhalte. Über eine zweite Busverbindung 19 ist der Speicher 11 weiterhin mit einer Auswahleinrichtung 14 verbunden. Sie ordnet den über den Datenbus 21 übertragenen Dateninhalte Speicherzellen 10 zu, in welche die Dateninhalte physikalisch abgelegt bzw. aus denen sie ausgelesen werden. Für die Zuordnung ist die Auswahleinrichtung 14 über einen zweiten Bus, den Adreßbus 20 ebenfalls mit dem Mikrocontroller 25 verbunden. Von ihm erhält die Auswahleinrichtung 14 in Form von logischen Adressen 23 über den Adreßbus 20 zu jedem Dateninhalt jeweils die Information, auf welche Speicherzelle 10 ein Zugriff erfolgen soll.

Die Auswahleinrichtung 14 beinhaltet weiterhin eine Verwürfelungseinrichtung 15. Diese ordnet den über den Adreßbus 20 zugeführten logischen Adressen 23 in unvorhersehbarer Weise Adressen 13 im Speicher 11 zu, auf die sodann tatsächlich physikalisch zugegriffen wird, d. h. die beschrieben bzw. ausgelesen werden. Die Zuordnung ist vorzugsweise jederzeit neu festlegbar. Zum Auslösen einer Neuordnung ist die Verwürfelungseinrichtung 15 über eine Steuerleitung 16 mit dem Mikrocontroller 25 verbunden.

Anhand einer beispielhaften Befehlssequenz wird im folgenden die Funktionsweise der vorbeschriebenen Anordnung erläutert. Die Befehlssequenz bestehe aus zwei, nicht notwendig unmittelbar aufeinanderfolgenden, Befehlen 27, 28, wovon der erste zunächst den Wert "1" in ein Register R2 legt und der zweite den Inhalt des Registers R2 zu einem späteren Zeitpunkt erneut aufruft, um ihn in ein "Ergebnisregister" genanntes Register zu schreiben.

Der erste Befehl 27 läßt sich symbolisch wie folgt darstellen: "MOV R2, #1"; darin steht "MOV" für die auszuführende Funktion Bewegen, R2 bezeichnet logisch die Adresse einer Speicherzelle 10 im Speicher 11, wohin die durch "#" gekennzeichnete Wert 1 gelegt werden soll. Die entsprechende symbolische Darstellung des zweiten Befehls 28 ist: "MOV erg, R2"; darin bezeichnet "MOV" wiederum die Funktion Bewegen, "erg" die logische Adresse 23 des Ergebnisregisters, R2 eine auszulesende Speicherzelle im Speicher 11. Die Befehlssequenz 27, 28 sei Teil eines Programmes bzw. einer nicht weiter dargestellten, umgreifenden Befehlsfolge 29, welche als Ganze z. B. zur Realisierung einer Funktion des Mikrocomputer oder einer durch den Mikrocomputer gesteuerten Einrichtung dient. Der Befehlsfolge 29 ist desweiteren ein Befehl 26 zum Starten einer Verwürfelung in der Auswahleinrichtung 14 vorangestellt. Dieser kann programmiert oder auch selbsttätig vom Mikrocontroller in Abhängigkeit von einem auslösenden Ereignis gebildet sein.

Bevor er mit der Ausführung der Befehlsfolge 29 beginnt, führt der Mikrocontroller 25 den Startbefehl 26 aus und bewirkt über die Steuerleitung 16 die Absetzung eines Signals zum Start der Verwürfelungseinrichtung 15. Das Startsignal löst in der Auswahleinrichtung 14 einen Verwürfelungsvorgang aus, durch den über den Adreßbus 20 übertragenen logischen Adressen 23 physikalische Adressen im Speicher 11 zugeordnet werden. Zweckmäßig wird durch die Verwürfelung allen möglichen logischen Adressen 23 jeweils eine Adresse 13 im Speicher 11 zugeordnet. Die durch die Verwürfelung erhaltene Zuordnung wird für die nachfolgende Abarbeitung der Programmsfolge 29 beibehalten, sie hat mithin auch für die Befehle 27, 28 Gültigkeit. Kommt somit der Befehl 27 zur Ausführung, übermittelt der Mikro-

controller 25 der Auswahlrichtung 14 über den Adreßbus 20 die logische Adresse R2. Die Auswahlrichtung 14 ermittelt hierauf die zugeordnete Speicherzelle 10 im Speicher 11. Es sei angenommen, daß die Verwürfelungseinrichtung 15 der logischen Adresse R2 im Speicher 11 physikalisch die Speicherzelle 10 mit der Adresse R5 zugeordnet habe. Die Auswahlrichtung ermittelt daher als der logischen Adresse R2 zugeordnete Speicherzelle die Zelle 10 mit der Adresse R5 und schreibt darein den mit dem Befehl 27 übermittelten Dateninhalt, d. h. den Wert 1.

Kommt anschließend die Ausführung der Befehlsfolge 29 an den Befehl 18, übermitteln der Mikrocontroller 25 der Auswahlrichtung 14 die logische Adresse 23 des Zielregisters, in diesem Fall die Adresse "erg" des Ergebnisregisters, sowie in symbolischer Angabe, was in das Zielregister zu laden ist, nämlich der Inhalt des Registers R2. Die Auswahlrichtung 14 ermittelt darauf wiederum die der logischen Adresse 23 R2 entsprechende physikalische Adresse 13 im Speicher 11, d. h. die Speicherzelle R5 und liest sodann deren Inhalt über den Datenbus 21 aus.

Ist die Programmfolge 29 abgearbeitet, kann unmittelbar erneut die Auslösung einer Zuordnungsverwürfelung durch die Verwürfelungseinrichtung 15, d. h. die Absetzung eines Startbefehles 26 vorgesehen sein. Selbst eine Mehrfachausführung derselben Programmfolge 28 ist dann mit einer regelmäßig wechselnden Belegung von Speicherzellen 10 im Speicher 11 verbunden. Alternativ kann ein erneuter Start der Verwürfelungseinrichtung 15 erst nach Durchführung mehrerer, etwa einer vorbestimmten Zahl von Programmfolgen 29 oder aber z. B. nur nach Neustart des Mikrocontrollers 25 vorgesehen sein.

Die Umsetzung der Erfindung ist unter Beibehaltung ihrer zugrundeliegenden Idee, nämlich die Zuordnung von physikalisch tatsächlich angesprochenen Adressen 13 im Speicher 11 zu in den Programmbefehlen verwendeten logischen Adressen 23 durch eine Verwürfelungseinrichtung unvorhersehbar zu machen, in einem weiten Rahmen variierbar. So kann ein anderer Speichertyp mit völlig anderer Gliederung gewählt werden oder die Verwürfelung von Zuordnungen sich auf Gruppen von Speicherzellen 10 beziehen. Anstelle eines gesonderten Adreßbusses 20 kann zur Übermittlung der logischen Adressen 23 an die Auswahlrichtung 14 ein anderes Verfahren gewählt werden. Zeitpunkt und Häufigkeit der Wiederholung der Verwürfelung durch die Verwürfelungseinrichtung 15 können ferner durch andere Ereignisse ausgelöst sein und auf andere Weise gesteuert werden. Anordnung wie Verfahren eignen sich desweiteren außer für die der Einfachheit halber zugrundegelegte serielle Befehlsabarbeitung in gleicher Weise etwa auch für nach objektorientierten Konzepten erstellte Programmbefehlsfolgen.

Patentansprüche

1. Speicheranordnung mit einem Speicher mit einer Vielzahl von Speicherzellen (10) sowie einer Auswahlrichtung (14), die aufgrund einer über einen Adreßbus (20) zugeführten logischen Adresse (23) eine Speicherzelle (10) auswählt, auf die anschließend ein physikalischer Zugriff erfolgt, **dadurch gekennzeichnet**, daß die Auswahlrichtung (14) eine Verwürfelungsvorrichtung (15) beinhaltet, die einer der Auswahlrichtung (14) übermittelten logischen Adresse (23) durch Verwürfelung in unvorhersehbarer Weise eine Speicherzelle (10) zuordnet und der anschließende physikalische Zugriff auf die zugeordnete Speicherzelle (10) erfolgt.
2. Speicheranordnung nach Anspruch 1, dadurch ge-

kennzeichnet, daß die Auswahlrichtung (14) einen Steuereingang (16) aufweist, über den die Verwürfelungsvorrichtung (15) startbar ist.

3. Speicheranordnung nach Anspruch 2, dadurch gekennzeichnet, daß die Auswahlrichtung (14) eine durch einen Verwürfelungsvorgang vorgenommene Zuordnung während der Abarbeitung einer ein Programm bildenden Befehlsfolge (29) beibehält.

4. Speicheranordnung nach Anspruch 1, dadurch gekennzeichnet, daß die Verwürfelungseinrichtung (15) auf ein Startsignal (26) hin jeweils für alle Zellen (10) in einem Speicher (11) eine Zuordnung zu logischen Adressen (13) vornimmt.

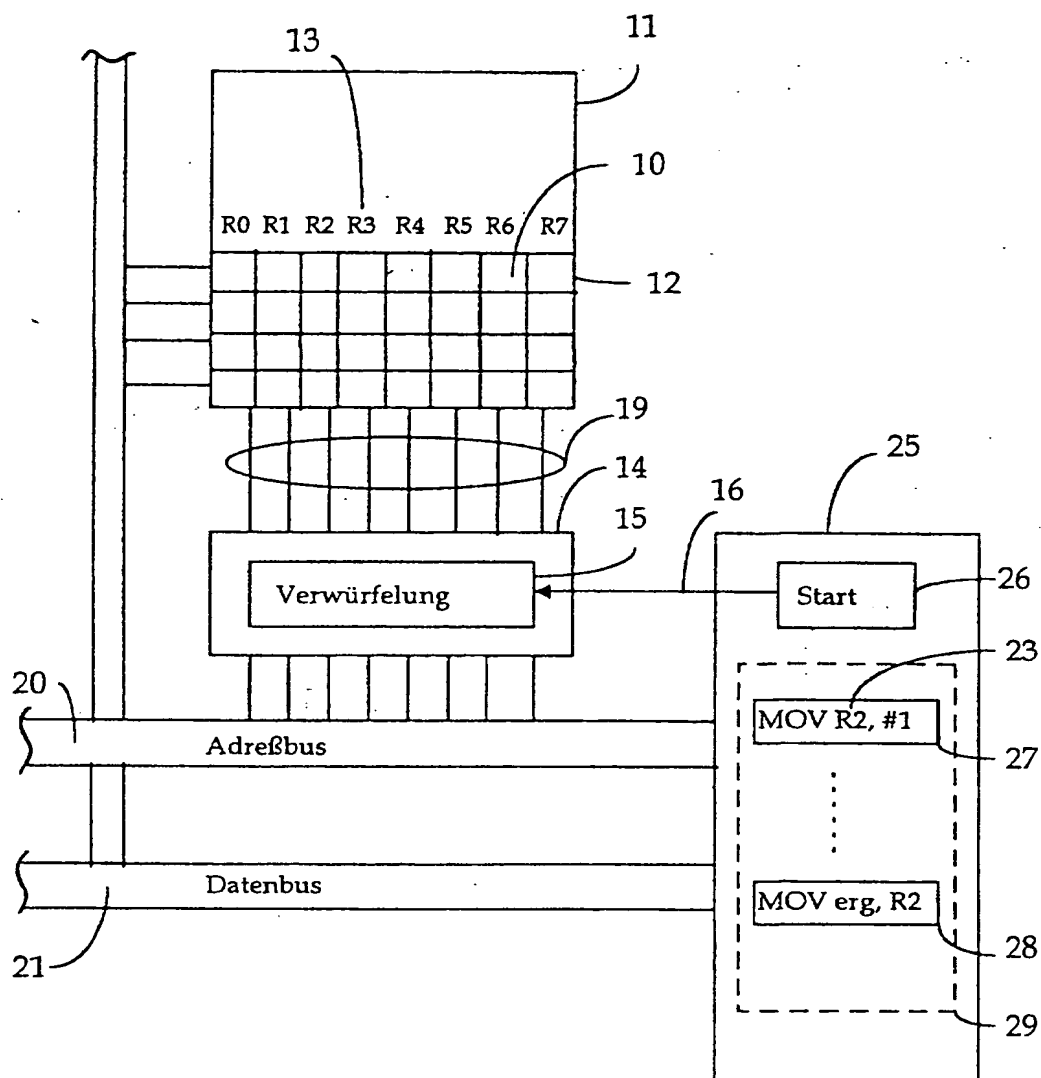
5. Speicheranordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Speicher (11) ein Speicher mit wahlfreiem Zugriff ist.

6. Speicheranordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Speicher (11) ein flüchtiger Speicher ist.

7. Verfahren zum Speichern von Dateninhalten in einen Speicher (11), wobei der Speicher (11) in Speicherzellen (10) gegliedert ist und die zu speichernden Daten jeweils einen Dateninhalt sowie eine logische Adresse (23) zur Bezeichnung einer Speicherzelle (10) im Speicher (11) enthalten, dadurch gekennzeichnet, daß aus der logischen Adresse (23) durch Verwürfelung die Adresse (13) einer Speicherzelle (10) gewonnen und der Dateninhalt in dem Speicher (11) physikalisch an der durch die Verwürfelung erzeugten Adresse (13) abgelegt wird.

8. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Zuordnung von logischen Adressen (23) zu physikalischen Adressen (13) im Speicher (11) durch Verwürfelung regelmäßig oder auf den Eintritt bestimmter Ereignisse hin wiederholt wird.

Hierzu 1 Seite(n) Zeichnungen



Figur